CLAIMS:

1. A method performed in a communication system including a plurality of nodes communicating in a shared network segment and at least one multicast channel in said shared network segment, the method comprising:

sending multicast messages from nodes on at least one multicast channel to other nodes;

providing a further specific multicast channel for sending start messages by the nodes to said other node;

sending a start message on said specific multicast channel by using a start nodes, wherein the start node starts an operation or an application;

receiving at a receiving node the start message; and

validating an authenticity of the start message upon receipt of the start message at the receiving node.

2. The method according to claim 1, wherein the step of sending the start message comprises monitoring by the start node for a predefined time to determine whether messages are sent on the specific multicast channel before sending the start message from the start node.

3. The method according to claim 1, wherein the step of sending the start message comprises signing or encrypting by the start node the start message using a key before sending the start message.

4. The method according to claim 3, wherein the step of sending the start message comprises using the key comprising a private key of the start node.

5. The method according to claim 1, further comprising:

providing two further multicast channels for exchanging other messages different from multicast start messages.

6. The method according to claim 1, wherein the step of sending the start message comprises using the start node to start the application comprising an Open Shortest Path First protocol.

7. The method according to claim 1, further comprising:

sending the multicast messages from the nodes comprising routers including a Designated Router and other routers;

deciding that the Designated Router comprises an only available node in a shared segment if the Designated Router does not receive a response or the start message from the other nodes when only the Designated Router comprises an active node in a shared network segment; and

generating a session key for at least one of authenticating or encrypting a further message by the Designated Router on another multicast channel when only the Designated Router comprises an active node in the shared network segment.

8. The method according to claim 7, wherein the step of generating comprises using at least one of the public/private key pairs of the Designated Router for generating the session key for at least one of authenticating or encrypting the further message.

9. The method according to claim 7, wherein the step of generating

comprises generating the session key as a function of a Random Number, a private key, a public key, and a TimeStamp.

10. The method according to claim 7, wherein the step of generating comprises using the session key as credential and applying the session key on a generated hello packet of an Open Shortest Path First protocol either for authentication or encryption.

11. The method according to claim 1, further comprising:

validating by the receiving node, when the receiving node receives the start message from another node on the specific multicast channel, the start message signed by a sending node; and

engaging in an Internet Key Exchange between the receiving node and the sending node to generate security associations.

12. The method according to claim 11, wherein the step of engaging comprises using one of the security associations for unicast communication between the nodes, and using another one of the security associations for multicast communication for transmitting messages.

13. The method according to claim 1, further comprising:

sending the multicast messages from the nodes comprising routers including a Designated Router, a Backup Designated Router and other routers;

engaging the Designated Router and the Backup Designated Router in an Internet Key Exchange with a new node to generate a unicast security association between the new node and the Designated Router and between the new node and the Backup Designated Router when the start message is sent

from the new node and both the Designated Router and the Backup Designated Router are active;

generating using the Designated Router a new key session for multicast communications; and

informing, using the Designated Router, the Backup Designated Router about the new session key using the unicast security association for communications between the Designated Router and the Backup Designated Router.

14. The method according to claim 1, further comprising:

generating a new session key for new nodes which connect and join an Open Shortest Path First network.

15. The method according to claim 1, further comprising:

providing a group communication mechanism, when a new node joins a group, an existing node leaves a group, group keys are changed, session keys are changed or new keys are distributed.

16. The method according to claim 1, further comprising:

generating using a Designated Router a new group key for all nodes when new Open Shortest Path First nodes join a network;

first distributing the new group key to a Backup Designated Router using the Designated Router ;

next using the Designated Router and the Backup Designated Router to distribute the new key to all other nodes using respective unicast security association messages.

17. A communication system comprising:

a plurality of nodes;

a shared network segment for communication between nodes of the plurality of nodes;

at least one multicast channel in said shared network segment on which the nodes can send multicast messages to other nodes;

a specific multicast channel on which the nodes can send start messages to the other nodes,

a start node for starting an operation or an application configured to send a start message on said specific multicast channel; and

a receiving node for receiving the start message configured to validate an authenticity of the start message.

18. The communication system according to claim 17 wherein said start node is configured to monitor for a predefined time to determine whether messages are sent on the specific multicast channel, before sending the start message from the start node.

19. The communication system according to claim 17, wherein the start node, before sending the start message, is configured to sign or encrypt the start message using a key.

20. The communication system according to claim 19, wherein the key used to sign the start message comprises a private key of this node.

21. The communication system according to claim 17, further comprising:

two further multicast channels to the specific multicast channel, for exchanging other messages different from multicast start messages.

22. The communication system according to claim 17, wherein the application comprises an Open Shortest Path First protocol.

23. The communication system according to claim 17, further comprising:

the nodes comprising routers including a Designated Router and other routers,

the Designated Router being configured, after sending the start message, to decide that the Designated Router comprises an only available node in a shared segment if the Designated Router does not receive a response or the start message from the other nodes when only the Designated Router comprises an active node in the shared network segment;

the Designated Router being configured to generate a session key for at least one of authenticating and encrypting a further message by the Designated Router on another multicast channel.

24. The communication system according to claim 23, wherein the Designated Router is configured to use at least one of a public or private key pair for generating the session key for at least one of authenticating and encrypting the further message.

25. The communication system according to claim 23, wherein the

session key is generated as a function of a Random Number, a private key, a public key, and a TimeStamp.

26. The communication system according to claim 23, wherein the session key is used as credential and is applied on a generated hello packet of an Open Shortest Path First protocol either for authentication or encryption.

27. The communication system according to claim 17, wherein when the receiving node receives the start message from another node on the specific multicast channel, the receiving node is configured to validate the received start message signed by the sending node, and the receiving node and the sending nodes then engage in an Internet Key Exchange to generate security associations.

28. The communication system according to claim 27, wherein one of the generated security associations is used for unicast communication between the nodes, and another one is used for multicast communications for transmitting messages.

29. The communication system according to claim 17, further comprising:

the nodes comprising routers including a Designated Router, a Backup Designated Router and other routers,

when a new node sends the start message and both the Designated Router and the Backup Designated Router are active, both the Backup Designated Router and the Designated Router are configured to engage in an Internet Key Exchange with the new node to generate a unicast security association for unicast communications between the new node and the

Designated Router, and between the new node and the Backup Designated Router,

the Designated Router is configured to generate a new session key for multicast communications and to inform the Backup Designated Router about the new session key using the unicast security association for communications between the Designated Router and the Backup Designated Router.

30. The communication system according to claim 17, wherein any new node which connects to and joins an Open Shortest Path First network receives a new session key.

31. The communication system according to claim 17, further comprising:

a group communication mechanism provided when a new node joins a group, an existing node leaves a group, session keys are changed and new keys or new keys are distributed.

32. The communication system according to claim 17, further comprising:

the Designated Router for generating a new group key for all nodes when new Open Shortest Path First nodes join a network;

the Designated Router configured to first distribute the new group key to a Backup Designated Router;

the Designated Router and the Backup Designated Router configured to, next, distribute the new group key to all other nodes using respective unicast security association messages.

33. A node for use in a system including at least one multicast channel on which the node can send multicast messages to other nodes, the node is configured to:

send a start message on a specific multicast channel of a system when the node starts an operation or an application.

34. The node according to claim 33 wherein said node, when starting the operation or the application, is configured to monitor for a predefined time to determine whether messages are sent on the specific multicast channel, before sending the start message from the node.

35. The node according to claim 33, wherein the node, before sending the start message, is configured to sign or encrypt the start message using a key.

36. The node according to claim 33, further comprising:

a routing comprising a Designated Router;

the Designated Router being configured, after sending the start message, to decide that the Designated Router comprises an only available node in a shared segment, if the Designated Router does not receive a response or the start message from other nodes; and

the Designated Router being configured to generate a session key for at least one of authenticating and encrypting a further message by the Designated Router on another multicast channel.

37. The node according to claim 33, wherein the node comprises a router.